2621
#3

Docket No. 197111US2SRD/vdm

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hirofumi MURATANI

GAU: 2621

SERIAL NO: 09/658,565

EXAMINER:

FILED: September 8, 2000

FOR: CODE GENERATING METHOD AND UNIT THEREOF, CODE DETECTING METHOD AND UNIT THEREOF, AND WATERMARK EMBEDDING UNIT AND WATERMARK DETECTING UNIT

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	11-280652	September 30, 1999
JAPAN	2000-016285	January 25, 2000
JAPAN	2000-263872	August 31, 2000

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

(B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.

Marvin J. Spivak
Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26,803

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

09/658,565

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ９月３０日

出 願 番 号
Application Number: 平成１１年特許願第２８０６５２号

出 願 人
Applicant (s): 株式会社東芝

２０００年 ６月 ９日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３０４４２５９

【書類名】　特許願

【整理番号】　A009905607

【提出日】　平成11年 9月30日

【あて先】　特許庁長官　殿

【国際特許分類】　G09C 5/00

【発明の名称】　電子透かし埋め込み装置及び電子透かし検出装置

【請求項の数】　8

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　村谷　博文

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子透かし埋め込み装置及び電子透かし検出装置

【特許請求の範囲】

【請求項１】

埋め込み対象コンテンツに対して透かし情報を埋め込む電子透かし埋め込み装置において、

入力された利用者識別番号に対して、複数の素数を法とする剰余をそれぞれ求める複数の剰余計算手段と、

前記複数の剰余計算手段により求められた剰余を表す符号であって、所定のビット数を一単位とする連続した１の列及び０の列で構成される部分符号をそれぞれ生成する複数の部分符号生成手段と、

前記複数の部分符号生成手段により生成された各部分符号を連接して前記透かし情報を生成する連接手段と、

生成された透かし情報を前記埋め込み対象コンテンツに埋め込む手段と

を具備することを特徴とする電子透かし埋め込み装置。

【請求項２】

透かし情報が埋め込まれた埋め込み済みコンテンツから透かし情報を検出する電子透かし検出装置において、

前記埋め込み済みコンテンツから所定のビット数を一単位とする連続した１の列及び０の列で構成される複数の部分符号を連接した連接符号からなる透かし情報を抽出する透かし情報抽出手段と、

抽出された透かし情報中の各部分符号を分割する符号分割手段と、

分割された各部分符号をそれぞれ復号して、それぞれに対して予め定められた素数を法とする２つの剰余からなる複数の剰余対を得る複数の部分符号復号手段と、

前記複数の剰余対の各一方の剰余から、利用者識別番号を計算により求める利用者識別番号計算手段と、

前記複数の剰余対から結託の有無を判定する結託判定手段と

を具備することを特徴とする電子透かし検出装置。

【請求項３】

前記結託判定手段により結託があると判定されたとき、前記複数の剰余対から計算により結託者を特定する結託者特定手段をさらに具備することを特徴とする請求項２記載の電子透かし検出装置。

【請求項４】

前記結託者特定手段は、ｋ′個の剰余対を入力し、各剰余対から一方の剰余を選択して、ｋ′個の剰余の組(ｒ１，ｒ２，…，ｒｋ′)を生成する剰余選択部と、

前記剰余選択部により生成されたｋ′個の剰余の組からｋ個の剰余(ｒ１，ｒ２，…，ｒｋ)を選択する一貫性選択部と、

前記一貫性選択部により選択されたｋ個の剰余から中国剰余定理に従って結託者番号候補を計算する中国剰余定理部とからなり、

前記一貫性検査部は、前記中国剰余定理部により計算された結託者番号ｕの候補と残りの(ｋ′－ｋ)個の剰余全ての間に、ｒｉ＝ｕ mod ｐｉ(ｉ＝ｋ＋１，…，ｋ′)が成立するか否かを判定し、この関係が成立する場合、ｕを結託者番号として出力し、この関係が成立しない場合には前記剰余選択部に対して、新たなｋ′個の剰余の組を要求し、結託者番号が特定できるまで新たな候補について同様の処理を繰り返すことを特徴とする請求項３記載の電子透かし検出装置。

【請求項５】

埋め込み対象コンテンツに対して利用者識別番号の情報を含む透かし情報を埋め込む電子透かし埋め込み装置において、

シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、

出力された符号語を前記透かし情報として前記埋め込み対象コンテンツに埋め込む手段と

を具備することを特徴とする電子透かし埋め込み装置。

【請求項６】

入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置において、

シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、

出力された符号語と前記コンテンツとの相関値を求める手段と、

前記相関値に基づいて前記コンテンツ中の前記入力された利用者識別番号に対応する符号語の有無を判定する手段と

を具備することを特徴とする電子透かし検出装置。

【請求項７】

入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置において、

予め登録された複数の利用者識別番号にそれぞれ対応する、シンプレックス符号を構成する複数の符号語を出力する手段と、

出力された各符号語と前記コンテンツとの各相関値を求める手段と、

求められた各相関値をベクトルとみなして計算されたノルムに基づいて前記コンテンツ中の透かし情報の有無を判定し、透かし情報があると判定した場合に前記相関値に基づいて結託者を特定する手段と

を具備することを特徴とする電子透かし検出装置。

【請求項８】

請求項１または５に記載の電子透かし埋め込み装置によって透かし情報が埋め込まれたコンテンツを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ディジタルデータ化された音声、音楽、動画、静止画等のコンテンツに対して透かし情報を埋め込む電子透かし埋め込み装置及び埋め込み済コンテンツから透かし情報を検出する電子透かし検出装置に関する。

【０００２】

【従来の技術】

電子透かし(digital watermarking)は、ディジタルデータ化された音声、音楽、動画、静止画等の著作権者や利用者の識別情報、著作権者の権利情報、そのデ

ータの利用条件、その利用時に必要な秘密情報、コピー制御情報などの情報(これらを透かし情報と呼ぶ)を知覚が容易ではない状態となるように埋め込み、後に必要に応じて透かし情報をそのデータ内から検出することによって利用制御、コピー制御を含む著作権保護を行ったり、二次利用の促進を行うための技術である。

【０００３】

[電子透かしの要件]

不正利用の防止を目的とする場合、電子透かし技術はディジタル著作物に対して通常に施されると想定される各種の操作や意図的な攻撃によって、透かし情報が消失したり改竄されたりしないような性質(ロバスト性)を持つ必要がある。例えば、静止画や動画はそれぞれＪＰＥＧ(Joint Photographic Coding Experts Group)符号化、ＭＰＥＧ(Moving Picture Experts Group)符号化と呼ばれる非可逆圧縮を施されることが多いため、電子透かし技術はこれらの非可逆圧縮に対するロバスト性を持つことが重要な要件となることが通常である。

【０００４】

[電子透かしの分類]

従来、画像に対する電子透かしの方式は、画素領域利用型と周波数領域利用型に大別することができる。画素領域利用型の電子透かし方式は、画素値を変更することで直接的に透かし情報の埋め込みを行うものである。一方、周波数領域利用型の電子透かし方式は、直交変換によって、一旦、画素領域から周波数領域へ移り、周波数領域において埋め込みを行った後、再び、逆直交変換によって周波数領域から画素領域に戻るものである。透かし情報は波として埋め込まれることになる。

【０００５】

[周波数領域利用型電子透かし方式]

周波数領域利用型の電子透かし方式としては、例えば文献[１] Koch, E. and Zhao, J., “Towards Robust and Hidden Image Copyright Labeling”, Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing, 452-455, June 20-22, 1995.(Koch-Zhaoの方式という)や、文献[２]Cox, I.J., Ki

lian, J., Leighton, T. and Shamoon, T., “Secure Spread Spectrum Watermarking for Multimedia”, NEC Research Institute, Technical Report 95-10, 1995.(Coxらの方式という)がある。これらの方式では、埋め込み対象となる周波数成分を非可逆圧縮による影響が小さな低周波数から中間周波数に設定することで非可逆圧縮に対するロバスト性を実現している。

〔０００６〕

[画素領域利用型電子透かし方式]

画素領域利用型の電子透かし方式としては、画素値のＬＳＢを変更することで埋め込みを行う方式がある。その変更は、擬似乱数系列(ＰＮ系列)に従って(文献[３] Schyndel, R.G. van, Tirkel, A.Z., and Osborne, C.F., “A Digital Watermark”, Proceedings of 1st IEEE International Conference on Image Processing, 1994.あるいは文献[４] Wolfganf, R.B. and Delp, E.J., “A Watermark for Digital Images”, ICIP96, 219-222, 1996.)、あるいは予め用意したマスクパターンに従って(文献[５] Pitas, I., “A Method for Signature casting on Digital Images”, ICIP96, 215-218, 1996.)、ある固定の大きさの変分を加えるか減ずるかを決定することで行う。この方式は、非可逆圧縮に対するロバスト性はあまり良くない。

〔０００７〕

[スペクトラム拡散による電子透かし]

スペクトラム拡散(spread spectrum)の考えを適用することで非可逆圧縮へのロバスト性を高める方式がある。スペクトラム拡散とは、通信したい信号に必要な帯域に比べて十分大きな帯域中に、情報を広く分散させて伝送する通信方式をいう(文献[６] 山内雪路, “スペクトラム拡散通信”, 東京電機大学出版局, 1994.)。伝送路上のノイズに対する耐性が優れている。元のコンテンツを搬送波、透かし情報を希望波、非可逆圧縮による影響を干渉波(ノイズ)とみなすことで、スペクトラム拡散の考えを電子透かし技術へ適用する。

〔０００８〕

スペクトラム拡散による電子透かし方式として、画素領域における拡散(文献[７] Smith, J.R. and Comiskey, B.O., “Modulation and Information Hiding

in Images”，Information Hiding，207-226，1996.、文献[８]大西淳児,岡一博,松井甲子雄，“PN系列による画像への透かし署名”，SCIS97，26B，1997.)と、周波数領域における拡散(先の文献[２]参照)が提案されている。文献[２]の方式と文献[８]の方式は、それぞれ摂動法、直接拡散法(direct sequence spread spectrum)と呼ばれることがある(文献[９] 松井甲子雄，“電子透かしの基礎－マルチメディアのニュープロテクト技術－”，森北出版株式会社,1998.)。

【０００９】

[周波数領域における拡散(摂動法)]

先の文献[１]の方式では、透かし情報の埋め込みは画素値に対して直交変換を行い、周波数領域において透かし情報を拡散して埋め込む。拡散は、周波数領域において複数の周波数成分の値とある乱数列に従って変化させることによって行う。拡散後、逆直交変換を行う。透かし情報の検出は、画素値に対して直交変換を行い、埋め込みが行われた周波数成分の値を埋め込みに用いられた乱数列の間の相関値によって判定を行う。埋め込まれた透かし情報は、画素領域では、画像(ブロック)全体に分散されているため、各種の操作に対してロバストである。また、透かし情報を埋め込んだ周波数成分が低中間周波数領域にあるならば、低周波数通過フィルタによっても透かし情報が失われにくい。

【００１０】

[画素領域における拡散(直接拡散法)]

一方、文献[８]の方式では、透かし情報の埋め込みは、ＰＮ(pseudo-random noise)系列を画素値に乗積することにより直接拡散する。得られた画像に対して直交変換を行い、周波数領域において透かし情報を埋め込み、再び逆直交変換を行う。その後、同じＰＮ系列を画素値に乗積して、逆拡散を行う。透かし情報の検出は、ＰＮ系列によって画素値を直接拡散する。得られた画像に対して直交変換を行い、透かし情報の埋め込みを行った周波数成分の値から判定する。直接拡散法では、画素値をＰＮ系列で変調するため、透かし情報は高周波成分に偏り、摂動法と比較して、ＪＰＥＧ圧縮等やＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ変換に対して、透かし情報が失われやすい。

【００１１】

[スペクトラム拡散の処理コストの軽減]

本発明者らは、ＪＰＥＧ圧縮等の下で透かし情報が失われにくくするために、透かし情報を埋め込むブロックサイズを大きくする方式を提案した(文献［１０］ 村谷博文,加藤拓,遠藤直樹，“直接拡散による電子透かしの耐性評価”，SCIS99，II，503-508，1999.)。

〔００１２〕

従来より、大きなブロックサイズの画像に対する埋め込みは行われていたが、この方式では大きなブロックに対する直交変換の処理コストを軽減することで埋込みおよび検出処理の低コストと高速性を実現した。この方式は、画像の周波数成分に依存しないか、あるいは、少数の周波数成分値にしか依存しない埋込み位置や埋込み強度を採用するため、揺動法よりも直接拡散法に適していた。しかし、この方式は大きなブロックサイズを選択したため、大きなサイズの透かし情報を埋め込むことが難しかった。

〔００１３〕

この問題に対しては、ブロック毎の画像の局所性に応じた埋め込みを行う「画像適応(image adaptation)」を行うによって、小さな埋込み強度によって埋め込みを行うことを可能にし、透かし情報のサイズを増加させる方法がある。例えば、文献［１１］Boland，F.M.，O Ruanaidh，J.J.K.，and Dautzenberg，C.，“Watermarking Digital Images for Copyright Protection”，Proceedings of the fifth International Conference on Image Processing and its Application，1995.(Boland等という)や、先の文献[８]に記載された方式で採用されている。

〔００１４〕

ところが、これら文献［１１］や先の文献[８]の方式では、埋め込み強度は多数の周波数成分の値から決定されるため、本質的に直交変換を避けることができなくなってしまう。従って、直交変換を行うことなく、画素値から直接に埋め込み強度を決定する方式をとることが望ましい。

〔００１５〕

[フィンガープリンティング]

大きなサイズの透かし情報をＪＰＥＧ圧縮等の対してロバストに埋め込むことができる電子透かし方式において、そのコンテンツ提供先の利用者を特定する情報を埋め込む応用形態が考えられる。このような応用形態は「フィンガープリンティング」と呼ばれる。海賊版の再配布を抑止する効果が期待できる。

【００１６】

[結託攻撃問題]

ところが、同じコンテンツに異なる透かし情報が埋め込まれた複数の埋め込み済みコンテンツが存在する場合、それら複数の埋め込み済コンテンツを利用して透かし情報を改竄、消失させるという行為が考えられる。このような行為は、「結託攻撃(collusion attack)」と呼ばれている。結託攻撃では、複数の埋め込み済みコンテンツの画素値を平均化することで新たなコンテンツを偽造したり、値が異なる画素値や周波数成分値の部分に対して、ランダムに、あるいは、多数決／少数決に従って値を変更する、などのやり方で改変を加える。

【００１７】

[結託攻撃に対する従来の対策]

従来、結託攻撃に対処する方法として、スペクトラム拡散による方法(先の文献[2]、及び文献［１２］山本哲也，渡辺創，嵩忠雄，“すべての結託ユーザを特定可能な電子透かし法”，SCIS'98，10.2.B，1998.)と、符号理論的な方法(文献［１３］ Boneh, Dan and Shaw, James, “Collusion-Secure Fingerprinting for Digital Data”，CRYPTO'95，452-465，1995.、文献［１４］鈴置昌宏，渡辺創，嵩忠雄，“結託攻撃に強い電子透かし法”，SCIS'97，31B，1997.及び文献［１５］ 吉田淳，岩村恵市，今井秀樹，“画質劣化が少なく結託攻撃に強い電子透かし法”，SCIS'98，10.2.A，1998.)が提案されている。

【００１８】

文献[2]の方法によれば、利用者毎にＮ(０，１)に従う相異なる実乱数列が与えられる。２つの異なる実乱数列の間に相関がないとする。結託攻撃は、画素値を平均化する操作とする。結託によって、検出時の相関値は減衰してしまう。

【００１９】

文献[2]では、相関値の代わりに、定義された類似度によって結託の検出を行

う。この類似度は、相関値を検出された透かし情報のノルムで除したものとして定義される。結託により電子透かしのノルムも減衰しているので、相関値が減衰しても類似度はさほど減衰しない。これにより結託者全員を特定することができる。ただし、この方法は検出において埋め込み対象であった原画像を必要とし、また結託者特定に時間がかかるのが難点である。

〔００２０〕

文献［１２］では、むしろ平均化による結託攻撃の際の相関値の減衰という性質を利用した結託者の特定方法を提案している。結託者間で共通の電子透かしは減衰せず、それ以外の電子透かしは減衰するので、埋め込み時のレベルを保っている電子透かしの組から結託者の組を特定する。全利用者数をｎ、想定する最大の結託者数をｃとすると、$(c+1)(c-1)\log_{c+1} n$オーダの長さの符号で結託者を特定することができる。ただし、この方法はスペクトラム拡散法に特有の性質を利用するため、すべての電子透かし方式に適用が可能なわけではない。

〔００２１〕

先の文献［１３］には、透かし情報を表現する符号において、すべての結託者の間で共通な値を持つビットは検出不能であるという性質を利用して、検出不能なビットがそのまま残るならば、それ以外のビットを如何に変更しようとも、結託者以外の利用者の符号を生成することができない符号(c-frameproof符号と呼ばれる)を構成して透かし情報とする方式が提案されている。

〔００２２〕

この方式では、誰のものでもない符号が生成される可能性は残るものの、これにより、ある利用者が自らのコンテンツをそのまま再配布した場合(native redistribution)、その利用者は他者の結託によるものであると主張しての否認はできなくなる。

〔００２３〕

結託者の総数に制限が無いn-frameproof符号は、符号サイズがｎとなる。結託者総数が最大cであるc-frameproof符号は、符号サイズが$16c^2 \log n$（ｃは結託者数、ｎは全利用者数)である。

〔００２４〕

文献［１３］ではさらに、２組の結託者のグループがあって、共通部分が空集合の場合、それぞれのグループ内での結託によって生成できる符号(feasible set)の集合間の共通部分も空集合であるような符号(totally c-secure符号)は存在しないということを示している。つまり、結託攻撃によって誰のものでもない符号を生成することができない符号は、厳密には存在しないことを示した。

〔００２５〕

そこで、文献［１３］では結託者数がｃ人以内の場合に結託者を誤って指摘する確率がε以下である符号(c-secure code with ε-error)を構成した。まず、誤りεを持つn-secure符号Γ(ｎ，２ｎ^2 log(２ｎ／ε))を構成した。その符号サイズは、２ｎ^2(n-1)log(2n/ε)である。

〔００２６〕

さらに、それをTraitor Tracingスキーム(文献［１６］Chor, B., Fiat, A. and Naor, M., “Tracing traitors”, Proceedings of CRYPTO'94, 257-270, 1994.)と組合せて誤りがε以下のc-secure符号の可能性を示した。この符号の符号サイズは、Ｏ(ｃ^4 log(ｎ／ε) log(１／ε))である。

〔００２７〕

[Chernoffの限界(Chernoff bound)]

文献［１６］では、Traitor Tracingスキームにおいて、Chernoffの限界の式を利用して結託者を特定するために必要な利用者固有鍵の数を決定している。先の文献［１３］では、その方法を流用して誤りεのn-secure符号やc-secure符号を構成した。平均値ｐの独立なｎ個の確率変数$X_i \in \{0, 1\}$があるとき、これらの和が平均値からずれる確率の限界を与えるのがChernoffの限界である。上端と下端の限界は、それぞれ次式で与えられる。

〔００２８〕

【数１】

$$\Pr\left[\sum_{i=1}^{n} X_i - np > n\delta\right] < \{\exp(\delta/p)/(1+\delta/p)^{1+\delta/p}\}^{np}$$

$$\Pr\left[\sum_{i=1}^{n} X_i - np < -n\delta\right] < \{\exp(-\delta/p)/(1-\delta/p)^{1-\delta/p}\}^{np}$$

【００２９】

さらに、緩い限界として次式が成り立つ。

【００３０】

【数２】

$$\Pr\left[\left|\sum_{i=1}^{n} X_i - np\right| > n\delta\right] < 2 \cdot \exp\{-\delta^2 n/(2p(1-p))\}$$

【００３１】

ここで、$0 \leqq \delta < p(1-p)$とする。また、次式が成り立つ。

【００３２】

【数３】

$$\Pr\left[\sum_{i=1}^{n} X_i - np < -n\delta\right] < \exp\{-\delta^2 n/(2p^2)\}$$

【００３３】

[結託者中の２人のみを指摘する方法]

文献［１３］で提案されている誤りεのn-secure符号やc-secure符号は、できるだけ多数の結託者を指摘するように設計されていた。利用者を順序集合とみなし、文献[４]で示されているΓ0(ｎ，ｄ)符号を結託者の集合の中から最大と最小の２人を特定する符号として利用することもできる。この場合には、より小さな符号サイズでの構成が可能である。

【００３４】

ここで、Γ0(n，d)符号とはｄビットを一単位とする連続した１の列及び０の列で構成される符号であり、このような１の列や０の列を符号数ｎに応じた単位数だけ並べて構成される。従って、この符号では１と０はそれぞれｄビットを体として連続するように配置され、ｄビット未満の数の１や０が孤立して存在することはない。

〔００３５〕

例えば、ｄ＝３，ｎ＝５とすれば、Γ0(n，d)符号であるΓ0(５，３)符号は以下のようになる。

１１１　１１１　１１１　１１１
０００　１１１　１１１　１１１
０００　０００　０００　１１１
０００　０００　０００　１１１
０００　０００　０００　０００

文献［１４］では、２つの符号を昇順と降順に重ね合わせた符号を利用し、結託者中の２人を特定するn-secure符号を提案している。この符号の符号サイズは、$2n\log_4(1/\varepsilon)=n\log_2(1/\varepsilon)$となる。文献［１５］では、Γ0(n，d)符号において０＜weight(ｘ｜Ｂs)となる最小のＳ(Ｓmin)と、weight(ｘ｜Ｂs)＜ｄとなる最大のＳ(Ｓmax)を求め、ＳminとＳmax＋１を結託者であると指摘するアルゴリズムによって結託者の２人を特定する方法を示した。この符号の場合、誤りεのn-secure符号は、符号サイズが$(n-1)\log_2(1/\varepsilon)$となる。

〔００３６〕

[誤りεの2-secure符号]

結託者総数が小さな場合には、符号サイズを小さくすることが可能である。先の文献［１５］には、結託者総数２人の場合に結託者の両方を指摘する符号であって、その符号サイズが$3n^{1/2}\log_2(1/\varepsilon)$の符号を示している。

〔００３７〕

[結託攻撃耐性の限界]

文献［１７］ Ergun, Funde, Joe Kilian and Ravi Kumar, “A Note on the Limits of Collusion-Resistant Watermarking”, EUROCRYPT'99, 140-149, 199

9.)は、電子透かし方式の詳細に依存せずに、結託攻撃に対する耐性には限界があることを理論的に示した。その主張は、正しい結託者を指摘する確率を高くしようとすると、誤った利用者を結託者として指摘してしまう確率(偽陽性率)が高くなってしまうというものであった。

【００３８】

文献［１７］で想定している結託攻撃は、図１５に示すように異なるすかし情報が埋め込まれた複数のコンテンツ(コンテンツ１，コンテンツ２，コンテンツ３)を平均化し、その後、ランダムな擾乱を加えるというものである。Ergun等の観点から、例えば先の文献［１３］での議論を捉えなおしてみる。文献［１３］における議論では、確率論的なc-secure符号の構成要素としてΓ0(ｎ，ｄ)符号を用いている。このΓ0(ｎ，ｄ)符号は、図１６(ｄ＝３の例)のように(1,1,1)と(-1,-1,-1)に符号をとる符号化をｎ重に直積して得られる。

【００３９】

このΓ0(ｎ，ｄ)符号に対して、文献［１７］で提案された結託攻撃を適用すると、平均化によって得られるコンテンツは、(1,1,1)と(-1,-1,-1)を結ぶ直線上にある重心に移る。結託攻撃は、さらに、その重心からずれた位置にコンテンツを移す。この場合、結託攻撃後のコンテンツが(1,1,1)か(-1,-1,-1)の近傍にある場合には、これは結託攻撃によって変更されていないと判断し、原点付近にある場合には結託攻撃によって変更されたとみなすことになる。

【００４０】

このΓ0(ｎ，ｄ)符号において、結託者のうち、(1,1,1)の符号を持つ者の数と(-1,-1,-1)の符号を持つ者の数の間に大きな偏りがある場合、平均化の結果、重心は(1,1,1)あるいは(-1,-1,-1)のかなり近くに位置することとなる。その後、ランダムな擾乱を受けるので、一般に、結託者を特定するアルゴリズムは、コンテンツが(1,1,1)または(-1,-1,-1)から擾乱によって移ったものか、重心から擾乱によって移ったものかを誤って判断する可能性が高い。つまり、Ergun等自身、かれらの結論がほとんどの電子透かしアルゴリズムに適用されると言明しているが、Boneh等の符号化もErgun等の限界を逃れることはできないといえる。

【００４１】

一方、Γ0(ｎ，ｄ)符号において、２つの符号間の最大距離はｎｄ、最小距離はｄと幅が大きい(図１７参照)。Γ0(ｎ，ｄ)符号は結託攻撃への耐性に重点がおかれいることから、受信空間中に非常にスパースに符号語が配置されているためである。

【００４２】

電子透かしアルゴリズムは、コンテンツの品質への影響がないように、符号間の最大距離ｎｄの符号を埋め込む必要がある。電子透かしアルゴリズムが、Γ0(ｎ，ｄ)符号をコンテンツ空間へ埋め込み、その埋め込みが、符号間の距離とコンテンツ間の距離とが比例するような性質を持つ場合、オリジナルのコンテンツとの透かし情報を埋め込んだ後のコンテンツとの間の最大距離もｎｄ／２以上となるので、ｎｄが大きな場合には、コンテンツ品質への影響が大きくなる(図１８の埋め込み１)。

【００４３】

仮に、これを避けるため、電子透かしアルゴリズムが符号をコンテンツ空間中のオリジナルコンテンツからの距離関係が保たれないような埋め込みによって、すべての符号語がオリジナルコンテンツとほぼ等しい距離にあるようにしたとすると、Γ0(ｎ，ｄ)符号がもともと持っていた結託攻撃への耐性の根拠が失われてしまうことになる(図１８の埋込み２)。

【００４４】

つまり、Ergun等の限界を意識した上で、結託攻撃に対する耐性の高さとコンテンツの品質への影響の小ささを適切に両立させた符号化による電子透かし方式を実現することが望ましいと考えられる。

【００４５】

(スペクトラム拡散による電子透かしの結託攻撃耐性)

一方、スペクトラム拡散による電子透かし方式では、埋め込みの影響がコンテンツ品質に大きな影響を与えないように埋め込み強度が設定される。その上で、埋め込みに用いる擬似乱数列が符号語に対応する。

【００４６】

標本値空間と周波数空間の間の直交変換は線形写像なので、攻撃対象の電子透

かし方式が空間領域利用型であれ周波数領域利用型であれ、Ergun等の結託攻撃は擬似乱数列を平均化して、さらに擾乱を与えるという操作となる。

【００４７】

スペクトラム拡散による電子透かし方式では、符号語である擬似乱数列は相互相関(cross-correlation)がほとんどゼロとなるように選択されることが普通である。従って、ｋ個のコンテンツの平均によって得られるコンテンツは、ある結託者に対応する擬似乱数列との相関が１／ｋに減衰すると考えられる。擬似乱数列間の相互相関が十分小さく、かつ、このｋがあまり大きくなければ、電子透かしの検出において相関値があるあらかじめ定められた閾値を越えるため、結託者を特定することが可能である。

【００４８】

前述した文献[２]の方式は、検出においてオリジナルコンテンツを利用することを前提としており、相関値の代わりに類似度(similarity)と呼ばれる量を用いて検出が行われる。類似度は、検出対象コンテンツからオリジナルコンテンツを引いた差分と埋め込みに用いた擬似乱数列の間の相互相関値を差分の自己相関値の平方根で正規化したものである。

【００４９】

類似度による検出では、結託攻撃における平均化によって、分子の相関値が１／ｋに減衰するが、分母の差分のノルムも１／ｋに減衰するため、類似度は減衰しないことが期待される。ただし、平均化以外にノイズが加わる場合には、そのノイズの影響は正規化によってかえって大きくなる。

【００５０】

文献［１８］ Kilian, Joe, F.Thomas Leighton, Lesley R. Matheson, Talal G. Shamoon, Robert E. Tarjan, and Francis Zane, “Resistance of Digital Watermarks to Collusive Attacks”, Technical Report TR-585-98, Department of Computer Science, Princeton University, 1998.では、統計的な議論によって文献[２]の電子透かし方式が何人までの結託者による結託攻撃に対する耐性を持っているかという理論的考察を行っている。疑似乱数系列はガウシアンノイズを仮定し、結託攻撃は結託者の持つコンテンツからオリジナルコンテンツを

統計的に推定することで行うと仮定する。その結果、現実的なパラメータ設定で、数名から十数名の結託者に対する耐性を実現することが可能であるという結論が得られている。

〔００５１〕

また、電子透かしの応用形態によっては、オリジナルコンテンツを用いた検出が行えず、検出対象コンテンツのみから検出を行う必要がある場合がある。その場合には、類似度による検出は行えない。この場合には、許容される結託者の数はさらに小さくなると考えられる。

〔００５２〕

ところで、文献[2]や文献［１８］での議論は、すべて、符号語である擬似乱数列の間の相互相関が十分小さいという前提に基づいている。しかし、一般に擬似乱数列の数が増えてくると、仮にそれをランダムに選択したとしても、偶然に大きな相互相関値を持つ対が生ずる可能性が高くなってくると思われる。

〔００５３〕

いったい、どの程度多くの擬似乱数系列が任意の対の間で相互相関値を小さくできるのか。また、そのような性質を持つ擬似乱数列をどのように選択すれば良いのか、そして、そのようにして選択された擬似乱数列を符号語として、どのような電子透かし方式を実現すれば、結託攻撃に強い方式となるのかが未解決の問題として残されている。

〔００５４〕

この問題も、先に[結託攻撃耐性]の項で述べた文献［１７］での限界を意識した上で、結託攻撃に対する耐性の高さとコンテンツの品質への影響の小ささを適切に両立させた符号化による電子透かし方式をどう実現させるかという問題の一つと考えられる。

〔００５５〕

相互相関の小さな２値の擬似ランダムビット列を生成する方法として、M系列を利用する方法が知られている。M系列は、線形フィードバックシフトレジスタ(ＬＦＳＲ)の出力として得られる系列のうち、ＬＦＳＲがＧＦ(２)の原始多項式の係数に対応するタップを持つ場合に生成されるものである。M系列中の１と０

をそれぞれ＋１と－１に置き換えると、ＰＮ系列となる。Ｍ系列は、０の出現頻度が１の出現頻度がほぼ等しく（１の出現頻度が一回少ない）、その間の相互相関関数は０のとき値１、０以外のとき－１／Ｌとなる。ここで、Ｌは系列の周期で、レジスタの段数をｎとすると、$L=2^{n}-1$である。

【００５６】

Ｍ系列から得られたＰＮ系列を巡回シフトして得られる系列を符号語として採用すれば、相互相関の小さな符号語が得られる。これらの符号語を電子透かしの埋め込みの際の擬似乱数系列として用いれば良い。この乱数系列は、空間領域利用型と周波数領域利用型の両方のスペクトラム拡散による電子透かしに利用できる。

【００５７】

周波数領域利用型のスペクトラム拡散の電子透かし方式では、普通、Ｎ（０，１）に従うガウシアンノイズを符号語とする。相互相関が小さな符号語を複数構成するには、逐次乱数列を生成し、それが、それまでに生成したすべての乱数列との相関が小さいことを確認し、仮に、大きな相互相関値を持つ場合には、その乱数列は符号語として採用しないという方法をとる。

【００５８】

しかし、この方法では、新たに生成した乱数列がそれまでに生成した乱数列と小さな相互相関であるという保証がないため、せっかく生成した乱数列を捨てなければならないことがあるため処理が無駄である。特に、乱数列の数がある程度以上増えると、その確率は高くなる。

【００５９】

【発明が解決しようとする課題】

以上に説明したように、従来の電子透かし技術では、結託攻撃によって透かし情報が失われたり偽造されたりすることで、不正な再配布が行われても、その不正行為者を特定できなくなる恐れがあった。

【００６０】

また、結託攻撃へのロバスト性を実現する従来の提案において、非常に冗長な形で透かし情報を埋め込む必要があるため、あまり大きな利用者総数や結託者数

を想定することができないという欠点があった。

〔００６１〕

特に、ＪＰＥＧ圧縮等やその他の攻撃への耐性を持つ電子透かしの埋め込み方式において、大きなサイズの透かし情報を埋め込むことはコンテンツの品質劣化を招く原因となる恐れがあった。

〔００６２〕

本発明の目的は、結託攻撃への耐性を有し、利用者総数や結託者総数が大きな場合においても、コンテンツの品質劣化を極力抑えて透かし情報を埋め込む電子透かし埋め込み装置及び電子透かし検出装置を提供することにある。

〔００６３〕

【課題を解決するための手段】

上記の課題を解決するため、本発明は埋め込み対象コンテンツに対して透かし情報を埋め込む電子透かし埋め込み装置において、入力された利用者識別番号に対して、複数の素数を法とする剰余をそれぞれ求める複数の剰余計算手段と、これらの各剰余計算手段により求められた剰余を表す符号であって、所定のビット数を一単位とする連続した１の列及び０の列で構成される部分符号をそれぞれ生成する複数の部分符号生成手段と、これらの各部分符号生成手段により生成された各部分符号を連接して透かし情報を生成する連接手段と、生成された透かし情報を埋め込み対象コンテンツに埋め込む手段とを具備することを特徴とする。

〔００６４〕

また、本発明は透かし情報が埋め込まれた埋め込み済みコンテンツから透かし情報を検出する電子透かし検出装置において、埋め込み済みコンテンツから所定のビット数を一単位とする連続した１の列及び０の列で構成される複数の部分符号を連接した連接符号からなる透かし情報を抽出する透かし情報抽出手段と、抽出された透かし情報中の各部分符号を分割する符号分割手段と、分割された各部分符号をそれぞれ復号して、それぞれに対して予め定められた素数を法とする２つの剰余からなる複数の剰余対を得る複数の部分符号復号手段と、複数の剰余対の各一方の剰余から、利用者識別番号を計算により求める利用者識別番号計算手段と、複数の剰余対から結託の有無を判定する結託判定手段とを具備することを

特徴とする。

【００６５】

この電子透かし検出装置においては、結託判定手段により結託があると判定されたとき、前記複数の剰余対から計算により結託者を特定する結託者特定手段をさらに具備してもよい。

【００６６】

本発明に係る他の電子透かし埋め込み装置は、埋め込み対象コンテンツに対して利用者識別番号の情報を含む透かし情報を埋め込む電子透かし埋め込み装置であって、シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、出力された符号語を透かし情報として埋め込み対象コンテンツに埋め込む手段とを具備することを特徴とする。

【００６７】

本発明の係る他の電子透かし検出装置は、入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置であって、シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、出力された符号語とコンテンツとの相関値を求める手段と、この相関値に基づいてコンテンツ中の入力された利用者識別番号に対応する符号語の有無を判定する手段とを具備することを特徴とする。

【００６８】

このような本発明に基づく電子透かし埋め込み／検出装置においては、透かし情報として埋め込むべき符号サイズを大きくすることなく、利用者総数や結託者数が大きくなっても、結託攻撃に対するロバスト性を得ることができる。

【００６９】

【発明の実施の形態】

図１は、本発明の電子透かし埋め込み装置１と電子透かし検出装置２が適用されるシステムの例であるフィンガープリンティングシステムの概念図を示す。

画像や音声などの埋め込み対象コンテンツと利用者識別番号が電子透かし埋め

込み装置１に入力され、ここで得られた埋め込み済みコンテンツがこれを格納する記憶媒体を含む流通経路３を経て流通する。

〔００７０〕

前述した結託攻撃は、流通経路３において埋め込みコンテンツに対して行われる。このような結託攻撃に対抗するために、本発明に基づく電子透かし検出装置２では、結託の有無を示す結託判定信号、結託があった場合の結託者を特定する結託者番号、及び結託がなかった場合の利用者識別番号が生成される。

〔００７１〕

以下、本発明による電子透かし埋め込み装置及び電子透かし検出装置の実施形態について説明する。

（第１の実施形態）

本発明の第１の実施形態として、従来例よりも小さな符号サイズを持つ誤りεのc-secure符号による電子透かし埋め込み装置及び電子透かし検出装置について説明する。

図２は、本発明の第１の実施形態に係る電子透かし埋め込み装置の概略構成を示している。この電子透かし埋め込み装置は、埋め込むべき透かし情報である利用者識別番号の埋め込み符号を生成する埋め込み符号生成部１１と、生成された埋め込み符号を埋め込み対象コンテンツに埋め込み、埋め込み済みコンテンツを得る符号埋め込み部１２とからなる。

〔００７２〕

図３は、埋め込み符号生成部１１の構成を示している。この埋め込み符号生成部１１は、それぞれｋ′個の法記憶部２１－１，２１－２，…，２１－ｋ′、剰余計算部２２－１，２２－２，…，２２－ｋ′、部分符号生成部２４－１，２４－２，…，２４－ｋ′と、符号パラメータ記憶部２３及び符号連接部２５からなる。

〔００７３〕

法記憶部２１－１，２１－２，…，２１－ｋ′には、相異なるｋ′個の素数ｐｉ(ｉ＝１，２，…，ｋ′)が法として記憶されており、剰余計算部２２－１，２２－２，…，２２－ｋ′は、入力される利用者識別番号ｕに対して、これらの素

数ｐiを法とする剰余ｕi＝ｕ mod ｐi(ｉ＝１，２，…，ｋ′)をそれぞれ求める。部分符号生成部２４－１，２４－２，…，２４－ｋ′は、ｋ′個の素数ｐi(ｉ＝１，２，…，ｋ′)に対して、符号パラメータ記憶部２３に記憶された符号パラメータｄに従って剰余計算部２２－１，２２－２，…，２２－ｋ′により求められた剰余ｕi(ｉ＝１，２，…，ｋ′)を表す前述したΓ0(ｎ，ｄ)符号からなる部分符号Γ(ｐi，１)をそれぞれ生成する。符号連接部２５は、部分符号生成部２４－１，２４－２，…，２４－ｋ′により生成された各部分符号Γ(ｐi，１)を連接することによって、透かし情報である埋め込み符号を生成する。

〔００７４〕

図４に、部分符号生成部２４－１，２４－２，…，２４－ｋ′の一つ(２４－ｉ)の構成を示す。符号パラメータをｄ、剰余をｕi、法をｐiとすると、減算部３１ではｐi－ｕi－１が求められる。“０”列生成部３２では、符号パラメータｄと剰余ｕiに基づきｄ×ｕiビットの連続した“０”列が生成され、“１”列生成部３３では、符号パラメータｄと減算部３１からの出力ｐi－ｕi－１に基づきｄ×(ｐi－ｕi－１)ビットの連続した“１”列が生成される。そして、これらの“０”列と“１”列が連接部３４で連接され、ｄ×(ｐi－１)ビットのビット列がΓ0(ｎ，ｄ)符号からなる部分符号Γ(ｐi，１)として生成される。

〔００７５〕

図５に、本実施形態に係る電子透かし検出装置の構成を示す。この電子透かし検出装置は、透かし情報抽出部４１、符号分割部４２、部分符号復号部４３－１，４３－２，…，４３－ｋ′、利用者識別番号計算部４４、結託判定部４５－１，４５－２，…，４５－ｋ′、結託判定ＯＲ部４６及び結託者番号計算部４７から構成されている。

〔００７６〕

透かし情報抽出部４１では、入力された埋め込み済みコンテンツから透かし情報(埋め込み符号)が抽出され、この抽出された透かし情報である埋め込み符号が符号分割部４２により各部分符号に分割された後、部分符号復号部４３－１，４３－２，…，４３－ｋ′により復号されることにより、利用者識別番号に対応する剰余対が生成される。

〔００７７〕

こうして生成された各剰余対の一方の剰余から、利用者識別番号計算部４４により利用者識別番号が計算で求められ、また各剰余対から結託判定部４５－１，４５－２，…，４５－ｋ′により結託の有無が判定される。結託判定部４５－１，４５－２，…，４５－ｋ′の判定結果について、結託判定ＯＲ部４６でＯＲがとられることにより、結託が存在したか否かが最終的に判定される。さらに、結託が存在すると判定されたときは各剰余対から結託者番号計算部４７で結託者番号が計算され、結託者が特定される。

〔００７８〕

図６に、結託者番号計算部４７の詳細な構成を示す。この結託者番号計算部４７は、ｋ′個の剰余対から各一つの剰余を選択する剰余選択部５１と、選択されたｋ′個の剰余のうちｋ個の剰余を選択する一貫性検査部５２、及びｋ個の剰余に対して中国剰余定理を適用して結託者番号候補を得る中国剰余定理部５３からなり、結託者番号候補が一貫性検査部５２にフィードバックされ、残りの(ｋ′－ｋ)個の剰余との間の一貫性検査が行われて、最終的に結託者番号が求められる。

〔００７９〕

本実施形態の電子透かし埋め込み装置及び電子透かし検出装置によると、利用者総数や結託者総数が大きい場合においても、コンテンツの品質劣化の少ない電子透かしが可能となる。以下、詳細に説明する。

利用者総数をｎとし、結託者総数の最大値をｃとする。一方、図３の法記憶部２１－１，２１－２，…，２１－ｋ′で用意されているｋ′個の素数ｐ1,ｐ2,…,ｐk′から任意のｋ個の素数を選んだとき、それらのｋ個の素数の積はｎ以上とする。例えば、この積はｎ≦ｐ1×ｐ2×…×ｐkである。

〔００８０〕

埋め込み符号生成部１２では、各素数ｐｉ(ｉ＝１，２，…ｋ′)に対して、図３の部分符号生成部２４－１，２４－２，…，２４－ｋ′により部分符号Γ(ｐｉ，１)が生成される。これらの部分符号Γ(ｐｉ，１)を符号連接部２５により連接することによって、新たな符号Γ(ｐ1,ｐ2,…,ｐk′：１)が生成される。

〔００８１〕

ここで、各利用者の利用者識別番号をｕとすると、その利用者識別番号ｕに対応する連接符号Γ(ｐ1,ｐ2,…,ｐk′:1)の符号語は、各部分符号Γ(ｐi, 1)がその利用者識別番号ｕに対する素数ｐiを法とする、剰余計算部２２－１，２２－２，…，２２－ｋ′で計算された剰余ｕ mod ｐiを表す符号語となり、これが透かし情報(埋め込み符号)として埋め込み対象コンテンツに埋め込まれることになる。

〔００８２〕

このようにして得られた埋め込み済みコンテンツに対して結託攻撃が行われた場合、図５の電子透かし検出装置において、符号分割部４２で分割された各部分符号Γ(ｐi, 1)を部分符号復号部４３－１，４３－２，…，４３－ｋ′することによって、ｃ人中のある２人の利用者識別番号のｐiに関する剰余(residue)の対が得られる。これをｐiに関する剰余対(residue pair)と呼ぶことにする。

〔００８３〕

また、ｐiに関する剰余対中のある剰余がある利用者識別番号ｕを保有する結託者ｕの剰余であるとき、その剰余は利用者識別番号ｕを保有する結託者に起因すると呼ぶことにする。このとき、この結託者を含めて結託者と同じ剰余の値を持つ利用者に関しては、その剰余はその利用者の利用者識別番号に起因する可能性があると呼ぶことにする。

〔００８４〕

(補題１)　ｃ人以下の結託において、Γ(ｐ1,ｐ2,…,ｐk′:1)によりｋ′個の相異なる素数に関する剰余対が与えられたとき、それらの剰余対中に、ある結託者の利用者識別番号に起因する剰余の数が２ｋ′／ｃ以上含まれるような結託者が少なくとも１人存在する。

〔００８５〕

(補題２)　剰余対中のある剰余に、結託により誤りを生じる確率をε以下とするには、$1 \geqq \log_2(1/\varepsilon)$でなければならない。

〔００８６〕

(系２′)　ｋ′個の剰余対に含まれる剰余のどの一つの剰余にも、結託によっ

て誤りが生じない確率をε以下とするには、$l \geqq \log_2(2k'/\varepsilon)$でなければならない。

【００８７】

（補題３） 符号Γ(p1,p2,…,pk′:1)は、結託により誤った符号を生じない確率をε以下とするには、$l \geqq \log_2(2k'/\varepsilon)$、つまり、符号サイズLは、次式でなければならない。

【００８８】

【数４】

$$L \geq \left(\sum_{i=1}^{k'} pi\right) \times \log_2(2k'/\varepsilon)$$

【００８９】

以下、pm=min(p1,…, pk′)、pM=max(p1,…, pk′)とし、また

【００９０】

【数５】

$$\langle p \rangle = \sum_{i=1}^{k'} pi/k'$$

【００９１】

とする。符号サイズの下限は、$L = k' \times \langle p \rangle \times \log^2(2k'/\varepsilon)$と表わされる。

【００９２】

（中国剰余定理(Chinese Remainder Theorem)）

相異なるk個の素数p1,p2,…,pkが与えられたとき、各i(i＝1, 2, …, k)についてui∈Zpiが与えられると、ui≡u mod piであるu∈$Z_{p1}\times Z_{p2}\times\cdots\times Z_{pk}$が一意に定まり、帰納的に計算できる。これが中国剰余定理である。

【００９３】

中国剰余定理を適用すると、図６に示すように中国剰余定理部５３にｋ′個の素数のうちｋ個の素数に対応する剰余が与えられれば、それから利用者識別番号を一意に定めることができる。しかし、それらの剰余すべてが同一結託者の利用者識別番号に起因するとは限らないため、求めた利用者識別番号が結託者を正しく特定するとは限らない。そこで、さらに第(ｋ＋１)番目の剰余を選択し、求めた利用者識別番号がこの剰余を与えるか否かで結託者を判定することとする。

〔００９４〕

結託者数が２人の場合については、この方法を比較的容易に実現できる(例えば、特願平１０－１０８０３９，特願平１０－１２２１０８)。ここでは、それを一般の結託者数に拡張する。

〔００９５〕

ｍ個の素数に対応する剰余の組(m-tuple of residues)の中の任意のｋ個の剰余に対して中国剰余定理を適用したとき、これらｍ個の剰余の組がすべて同一の利用者識別番号を与える場合、このような剰余の組を一貫している(consistent)と呼ぶことにする。図６の一貫性検査部５２では、剰余選択部５１でｋ′個の剰余対から各一つ選択されたｋ′個の剰余を入力し、これらｋ′個の剰余の中からｍ個の剰余を選択し、さらに一貫性検査を行ってｋ個の剰余を選択して中国剰余定理部５３に引き渡す。

〔００９６〕

さらに、このような一貫している剰余の組のすべての剰余が、求められた結託者の利用者識別番号に起因している場合、この剰余の組は真に一貫している(truly consistent)と呼び、そうでない場合、この剰余の組は偽って一貫している(falsely consistent)と呼ぶことにする。このような偽って一貫している組の簡単な例を以下に挙げる。

一貫しているｍ個の剰余に対して、さらに第(ｍ＋１)番目の素数ｐに関する剰余を加えて(ｍ＋１)個の剰余としたとき、それらが一貫している確率は、新たに加えた素数ｐに関する剰余がランダムに値をとる場合には、１／ｐとなる。

〔００９７〕

従って、ｍ個の剰余対から各１個の剰余を選択して、ｍ個の剰余を構成する場

合、偶然に、偽って一貫したｍ個の剰余が得られる確率は、ｍを大きくするにつれて小さくなり、その確率は$(2/p_m)^{m-k}$より小さくなる。ただし、ｍ＞ｋとする。

〔００９８〕

（補題４） 偽って一貫した剰余の組が得られる確率をε以下とするには、$m \geqq k+\log_{p_m/2}(1/\varepsilon)$とすればよい。

ここで、（系４）から、偽って一貫した剰余の組が得られる確率をε以下とするためには、$m \geqq k+\log_{p_m/2}(1/\varepsilon)$個の同一利用者に起因する剰余を含む剰余対を用意すれば良い。（補題１）から、それには$k' \geqq (c/2)\times(k+\log_{p_m/2}(1/\varepsilon))$の剰余対を用意すれば良い。

〔００９９〕

結託者を正しく決定するには、剰余対が正しく得られた上で真の一貫した組を得る必要がある。そこで、それぞれの誤り確率εをε′と以下とすると、結託者を正しく決定できない確率は$(\varepsilon+\varepsilon')$以下となる。そこで、$\varepsilon \rightarrow \varepsilon/2$、$\varepsilon' \rightarrow \varepsilon/2$と再定義して、次の定理を得る。

〔０１００〕

（定理） 符号$\Gamma(p1,p2,\cdots,pk':1)$が、誤り確率ε以下で結託者を正しく決定するには、$k' \geqq (c/2)\times(k+\log_{p_m/2}(2/\varepsilon))$、$1 \geqq \log_2(4k'/\varepsilon)$を満たせば良い。

よって、（補題３）よりその符号サイズの下限は、

$$L=\langle p\rangle\times(c/2)\times(k+\log_{p_m/2}(2/\varepsilon))\times\log_2((2c/\varepsilon)\times(k+\log_{p_m/2}(2/\varepsilon)))$$

で与えられる。

〔０１０１〕

ここで、すべての素数がほぼ同じ大きさとなるように選択する。$p_i \fallingdotseq p$とすると、$p \fallingdotseq \langle p\rangle \fallingdotseq n^{1/k}$。よって、符号サイズの下限は、

$$L \fallingdotseq (c/2)\times n^{1/k}\times(k+\log_{n^{1/k}/2}(2/\varepsilon))\times\log_2((2c/\varepsilon)\times(k+\log_{n^{1/k}/2}(2/\varepsilon)))$$

で近似される。

〔０１０２〕

さらに、ある正数ａを選び、$k=(\log_2 n)/a$と設定することができるならば、符号サイズの下限は、

$$L \fallingdotseq (c e^a/2a)\times(\log_2 n + a\times\log_e a/2(2/\varepsilon)) \times\log_2((2c/\varepsilon a)\times(\log_2 n + a\times\log_e a/2(2/\varepsilon)))$$

で近似される。この場合、符号サイズの下限はｃに関して$\Theta(c\log_2 c)$、ｎに関して$\Theta(\log_2 n \log_2\log_2 n)$となり、例えば先の文献[１４]や文献[１５]に開示された従来の方式と比較して、最も小さなオーダーとなる。

(素数定理(prime number theorem))

自然数ｘを超えない素数の個数を$\pi(x)$とすると、$\pi(x)\fallingdotseq x/\log x$となる。先ほどの符号化では、$k=(\log_2 n)/a$とした。そこで、素数定理よりδを小さな正数とするとき、ｘ～ｘ(１＋δ)の間に素数が$\log_2 x$オーダーの個数以上存在することは、次のように確認できる。

〔０１０３〕

$$\pi(x+(1+\delta))-\pi(x)\fallingdotseq(x/(\log x-1)/\log^2 x) = \omega(\log x)$$

次に、上の定理が前提としている、結託者を特定するアルゴリズムについて図７に示すフローチャートを用いて説明する。

結託者番号計算部４７は、部分符号復号部４３－１，４３－２，…，４３－ｋ′が出力したｋ′個の剰余対を入力する(ステップＳ１)。剰余対は、まず剰余選択部５１に入力される。剰余選択部５１は、各剰余対から一方の剰余を選択し、ｋ個の剰余の組(ｒ１，ｒ２，…，ｒｋ′)を生成する(ステップＳ２)。

〔０１０４〕

生成されたｋ′個の剰余の組は、一貫性検査部５２に入力される。一貫性検査部５２は、入力されたｋ′個の剰余の組からｋ個の剰余(ｒ１，ｒ２，…，ｒｋ)を選択し(ステップＳ３)、中国剰余定理部５３に渡す。

〔０１０５〕

中国剰余定理部５３は、中国剰余定理に従い結託者番号ｕを計算する(ステップＳ４)。この中国剰余定理の計算は、図８のフローチャートに示す処理の流れ

に従って行われる。計算された結託者番号ｕは、一貫性検査部５２へ返される。

〔０１０６〕

一貫性検査部５２では、残りの(ｋ′－ｋ)個の剰余全てとｕとの間に、ｒｉ＝ｕ mod ｐｉ(ｉ＝ｋ＋１，…，ｋ′)が成立するか否かを判定する(ステップＳ５)。この関係が成立する場合、一貫性検査部５２はｕを結託者番号として出力する(ステップＳ６)。この関係が成立しない場合には、一貫性検査部５２は剰余選択部５１に対して、新たなｋ′個の剰余の組を要求する(ステップＳ７)。もし、新たな候補が存在しない場合には、結託者番号の特定に失敗したことになる(ステップＳ８)。

〔０１０７〕

最後に、図９に示すフローチャートを用いて本実施形態における電子透かし検出装置の処理の流れについて説明する。

埋め込み済みコンテンツが入力され(ステップＳ１１)、この埋め込み済みコンテンツから透かし情報抽出部４１で透かし情報である埋め込み符号が検出されると(ステップＳ１２)、符号分割部４２及び部分復号部４３－１，４３－２，…，４３ｋ′を介して得られた部分符号に基づいて、結託判定部４５－１，４５－２，…，４５－ｋ′により結託の有無が判定される(ステップＳ１３)。

〔０１０８〕

ここで、結託判定部４５－１，４５－２，…，４５－ｋ′のいずれでも結託が無いと判定されると、利用者識別番号計算部４４により利用者識別番号が計算され(ステップＳ１４)、この利用者識別番号が出力される(ステップＳ１５)。

〔０１０９〕

一方、ステップＳ１３で結託判定部４５－１，４５－２，…，４５－ｋ′の少なくとも一つで結託が有ると判定されると、結託判定部４６を介して結託存在信号が出力され(ステップＳ１６)、かつ結託者番号計算部４７で結託者番号が計算され(ステップＳ１７)、この結託者番号が出力される(ステップＳ１８)。

〔０１１０〕

この場合、ステップＳ１３での結託の有無の判定と、ステップＳ１４での利用者識別番号の計算については、処理が簡単であり、高速に行うことができる。こ

れに対して、ステップＳ１７での結託者番号の計算には時間がかかるが、結託の有無の判定を先に行い、結託が有ったと判断された場合にのみ結託者番号の計算を行うことにより、無駄な計算を省略できる。

【０１１１】

また、本発明の電子透かし検出装置を利用者機器に適用する場合には、結託の有無のみを判定し、その結果によって利用を中断させるなどの利用制御を行えばよいので、結託者の計算(特定)まで行う必要は必ずしもない。

【０１１２】

このように本実施形態によると、埋め込むべき符号サイズを抑えつつ、利用者総数や結託者数が大きい場合についても、結託攻撃に対するロバスト性を持つことができる。

【０１１３】

(第２の実施形態)

次に、本発明の第２の実施形態として、埋め込み済みコンテンツの品質への影響を小さく抑えるように、従来よりも最適な符号化が行われる電子透かし埋め込み装置及び検出装置について説明する。

【０１１４】

図１１に、本実施形態に係る電子透かし埋め込み装置の構成を示す。この電子透かし埋め込み装置は、シンプレックス符号生成部６１、符号語選択部６２及び電子透かし埋め込み部６３から構成されている。

【０１１５】

シンプレックス符号とは、符号長ｎ－１、符号語数ｎで、符号語間の相互相関が－１／(ｎ－１)となる符号であり、ｎ次のアダマール(Hadamard)行列を基に構成することができる。すなわち、符号語がｎ－１次元ユークリッド空間中のｎ－１次元単体の頂点に位置するような符号がシンプレックス符号である。例えば、３次元ユークリッド空間の場合は、図１０に示すように(-1,-1,1)，(1,-1,-1)，(-1,1,-1)で示す３つの頂点に位置する符号がシンプレックス符号を構成する。

【０１１６】

シンプレックス符号生成部６１では、このようなシンプレックス符号の符号語

を生成する。シンプレックス符号生成部６１は、あらかじめ生成された符号語の表を記憶したものであってもよい。符号語選択部６２は、生成されたシンプレックス符号に順番を割り振っておき、与えられた利用者識別番号に対応する符号語を選択して出力する。なお、シンプレックス符号生成部６１及び符号語選択部６２の部分は、利用者識別番号が入力されてから、利用者識別番号に対応するシンプレックス符号の符号語を生成して出力するように構成されていてもよい。

【０１１７】

電子透かし埋め込み部６３は、符号語選択部６２より受け取った符号語を透かし情報として埋め込み対象コンテンツに埋め込む。埋め込みは、スペクトラム拡散によって行う。

【０１１８】

図１２に、図１１に示した電子透かし埋め込み装置に対応する本実施形態に係る電子透かし検出装置の構成を示す。この電子透かし検出装置は、シンプレックス符号生成部７１、符号語選択部７２、相関値計算部７３及び相関値判定部７４から構成されている。シンプレックス符号生成部７１と符号語選択部７２については、図１１で説明した電子透かし埋め込み装置の中のそれと同一であるため、説明を省略する。

【０１１９】

相関値計算部７３では、入力された埋め込み済みコンテンツと入力された利用者識別番号に基づいて符号選択部７２で選択された符号語との間の相関値を計算する。相関値判定部７４では、相関値計算部７３により計算された相関値がある閾値を超えているか否かによって、符号選択部７２からの符号語が埋め込み済みコンテンツに埋め込まれているか否かを判定し、検出／非検出信号を出力する。

【０１２０】

このように本実施形態に係る電子透かし埋め込み／検出装置によれば、任意の対の間での相互相関値が小さくなるようなシンプレックス符号の符号語を擬似乱数系列として用い、これを透かし情報として埋め込んでいる。従って、透かし情報として別の利用者識別番号に対応する符号語が埋め込まれていると誤判定を行う確率は非常に小さくなる。

【０１２１】

（第３の実施形態）

次に、本発明の第３の実施形態として、第２の実施形態の電子透かし検出装置を応用して結託攻撃に対する結託者特定機能を持たせた電子透かし検出装置ついて説明する。図１３は、本実施形態に係る結託者特定機能に係る部分の構成を示している。

【０１２２】

この電子透かし検出装置は、結託者特定機能を持たせるために、シンプレックス符号生成部８１、符号語選択部８２、相関値計算部８３、利用者識別番号生成部８４、相関値ベクトルノルム計算部８５、電子透かし判定部８６及び結託者判定部８６を有する。シンプレックス符号生成部８１、符号語選択部８２及び相関値計算部８３は、図１２に示した電子透かし検出装置の中のそれと基本的に同じである。

【０１２３】

利用者識別番号生成部８４では、予め登録されたすべての利用者識別番号を生成する。符号語選択部８２では、これらすべての利用者識別番号に対応するシンプレックス符号の符号語が選択され、これらの各符号語と図示しない埋め込み済みコンテンツとの相関値が相関値計算部８３で計算される。

【０１２４】

相関値ベクトルノルム計算部８５では、すべての利用者識別番号に対して計算された相関値をベクトルとみなして、そのノルムを計算する。この相関値ベクトルノルムは、例えばすべての相関値の和とする。

【０１２５】

電子透かし判定部８６では、計算されたベクトルノルムに基づいて、例えば、このノルムがある閾値を超えるか否かにより、透かし情報が埋め込まれていたか否かを判定する。この判定の結果、透かし情報が埋め込まれていたと判断した場合には、結託者判定部８７において相関値ベクトルの中で最も大きな値を示した利用者識別番号を保有する利用者を結託者として特定する。

【０１２６】

また、結託者特定部８７においては、このような方法の他、例えば相関値ベクトルがｎ－１次元単体の部分単体のうち、どの部分単体の重心を通るかを求め、その部分単体の頂点に対応する利用者識別番号を保有する利用者を結託者とすることで、複数の結託者を特定することもできる。

【０１２７】

なお、第２乃至第３の実施形態において、透かし情報として用いる擬似乱数系列として、Ｎ(０，１)のガウシアンノイズを採用する場合には、図１４に示すようにシンプレックス符号生成部９１で生成されたシンプレックス符号をランダム座標回転部９２によりランダムに回転させて符号語とすればよい。

【０１２８】

【発明の効果】

以上説明したように、本発明によればフィンガープリンティングシステムを構成する電子透かし埋め込み／検出装置において、利用者総数や結託者数が大きくなっても、小さな符号サイズの透かし情報を埋め込ことによってコンテンツの品質劣化を伴うことなく、結託攻撃に対するロバスト性を持つことができ、非可逆圧縮等の他の攻撃に対してもロバスト性を得ることができる。

【０１２９】

また、本発明の電子透かし埋め込み／検出装置により、コピー制御情報や利用制御情報といった透かし情報を埋め込み、コンテンツを利用する機器を制御する場合に、同一コンテンツに対して異なる機器制御情報が埋め込まれている場合にその比較によって制御情報の改竄を行う攻撃に対してもロバスト性を有するコンテンツ利用システムを構築することも可能である。

【図面の簡単な説明】

【図１】　本発明に係る電子透かし埋め込み装置及び電子透かし検出装置が適用されるフィンガープリンティングシステムの概略構成を示す図

【図２】　本発明の第１の実施形態に係る電子透かし埋め込み装置の構成を示すブロック図

【図３】　図２における埋め込み符号生成部の構成を示すブロック図

【図４】　図３における部分符号生成部の構成を示すブロック図

【図５】　本発明の第１の実施形態に係る電子透かし検出装置の構成を示すブロック図

【図６】　図５における結託者番号計算部の構成を示すブロック図

【図７】　同実施形態における結託者特定アルゴリズムを示すフローチャート

【図８】　図５における中国剰余定理部の処理の流れを示すフローチャート

【図９】　同実施形態に係る電子透かし検出装置の処理の流れを示すフローチャート

【図１０】　本発明の第２乃至第３の実施形態で使用するシンプレックス符号について説明する図

【図１１】　本発明の第２の実施形態に係る電子透かし埋め込み装置の構成を示すブロック図

【図１２】　本発明の第２の実施形態に係る電子透かし検出装置の構成を示すブロック図

【図１３】　本発明の第３の実施形態に係る結託者特定機能を有する電子透かし検出装置の構成を示すブロック図

【図１４】　本発明の第２乃至第３の実施形態におけるシンプレックス符号生成部の他の例を示すブロック図

【図１５】　電子透かしに対する結託攻撃について説明する図

【図１６】　Γ0(n，d)符号及びそれに対する結託攻撃を説明する図

【図１７】　Γ0(n，d)符号における二つの符号間の最大距離と最小距離について説明する図

【図１８】　Γ0(n，d)符号を用いた従来の電子透かしアルゴリズムにおける問題点を説明する図

【符号の説明】

１１…埋め込み符号生成部

１２…符号埋め込み部

２１－１，２１－２，…，２１－k′…法記憶部

２２－１，２２－２，…，２２－k′…剰余計算部

２３…符号パラメータ記憶部

２４－１，２４－１，…，２４－ｋ′…部分符号生成部

２５…符号連接部

４１…透かし情報抽出部

４２…符号分割部

４３－１，４３－２，…，４３－ｋ′…部分符号復号部

４４…利用者識別番号計算部

４５－１，４５－２，…，４５－ｋ′…結託判定部

４６…結託判定ＯＲ部

４７…結託者番号計算部

６１…シンプレックス符号生成部

６２…符号語選択部

６３…電子透かし埋め込み部

７１…シンプレックス符号生成部

７２…符号語選択部

７３…相関値計算部

７４…相関値判定部

８１…シンプレックス符号生成部

８２…符号語選択部

８３…相関値計算部

８４…利用者識別番号生成部

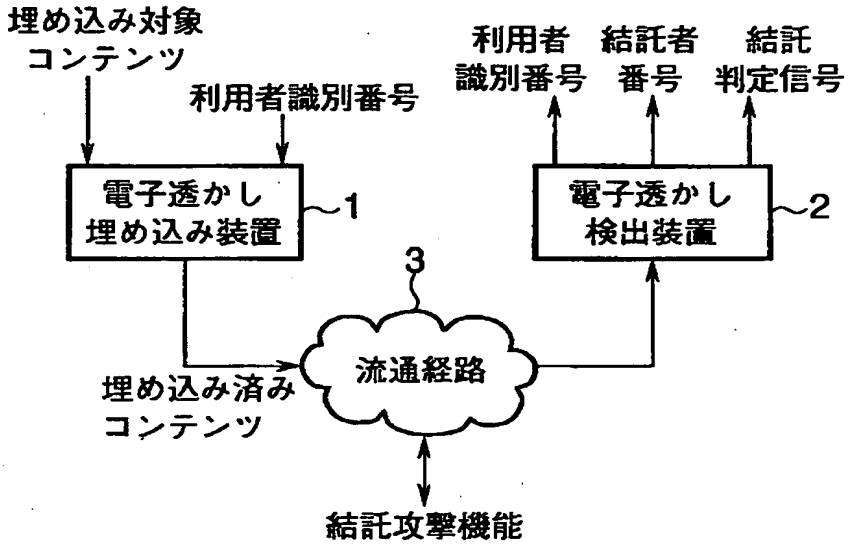
８５…相関値ベクトルノルム計算部

８６…電子透かし判定部

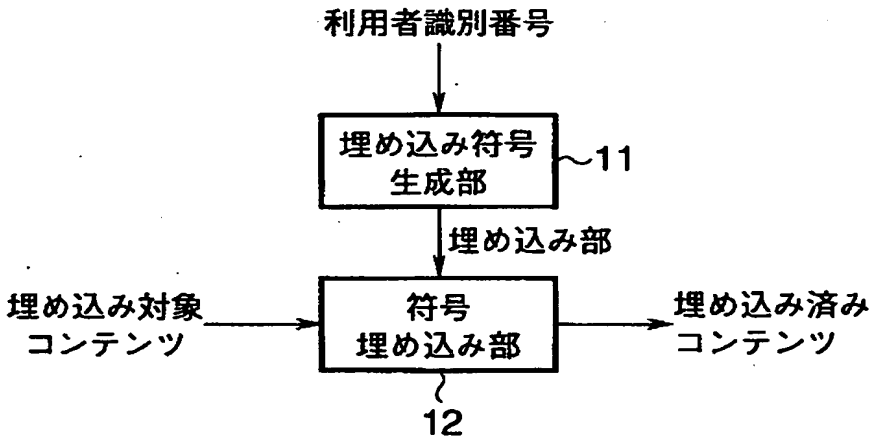
８７…結託者特定部

【書類名】　図面

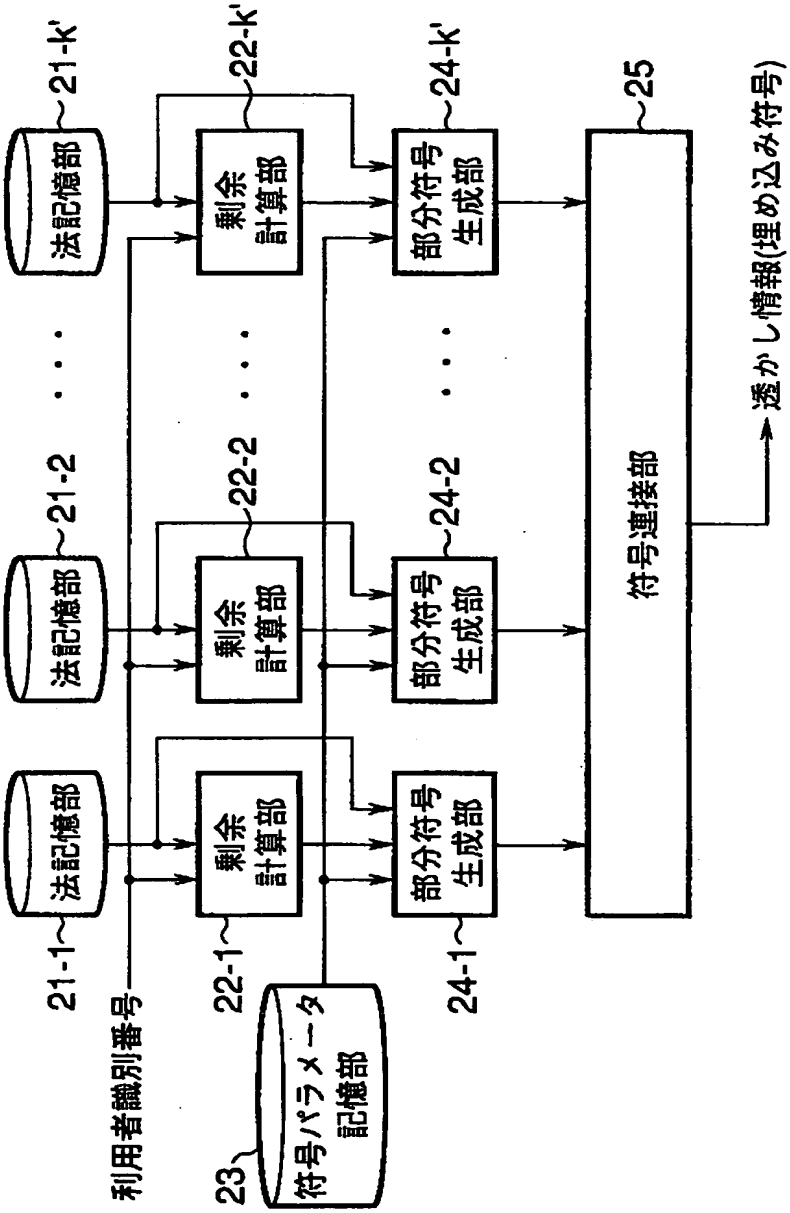
【図１】


埋め込み対象
コンテンツ
利用者識別番号
利用者
識別番号
結託者
番号
結託
判定信号
電子透かし
埋め込み装置
1
電子透かし
検出装置
2
3
流通経路
埋め込み済み
コンテンツ
結託攻撃機能

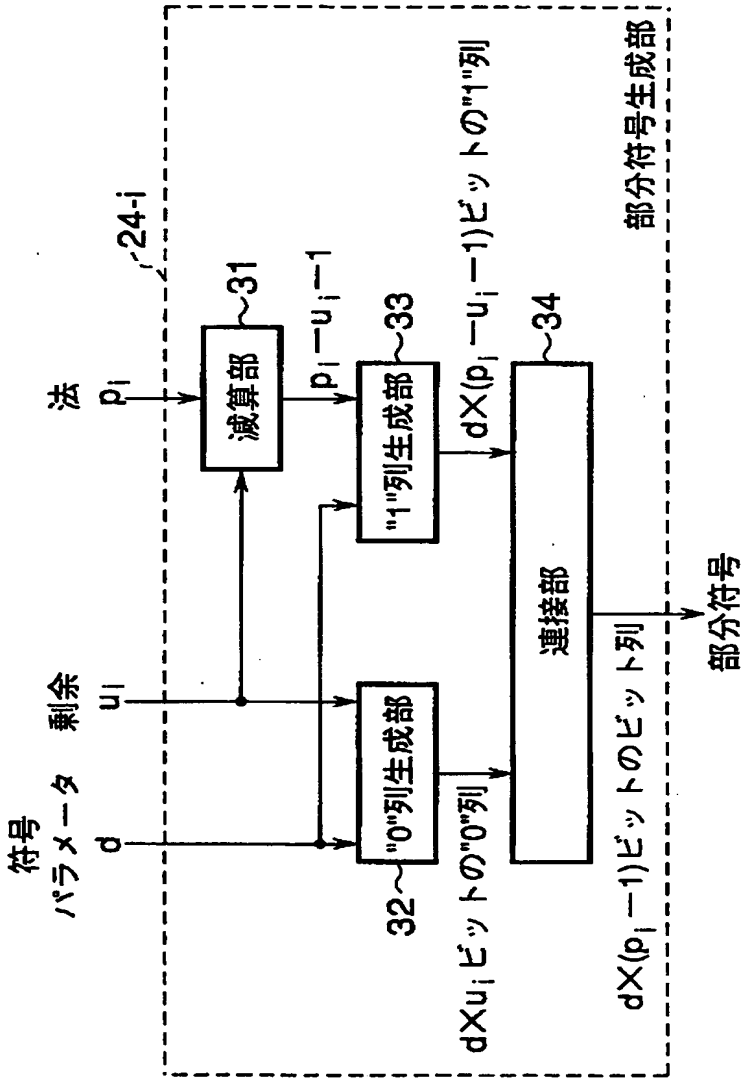
【図２】


利用者識別番号
埋め込み符号
生成部
11
埋め込み部
埋め込み対象
コンテンツ
符号
埋め込み部
埋め込み済み
コンテンツ
12

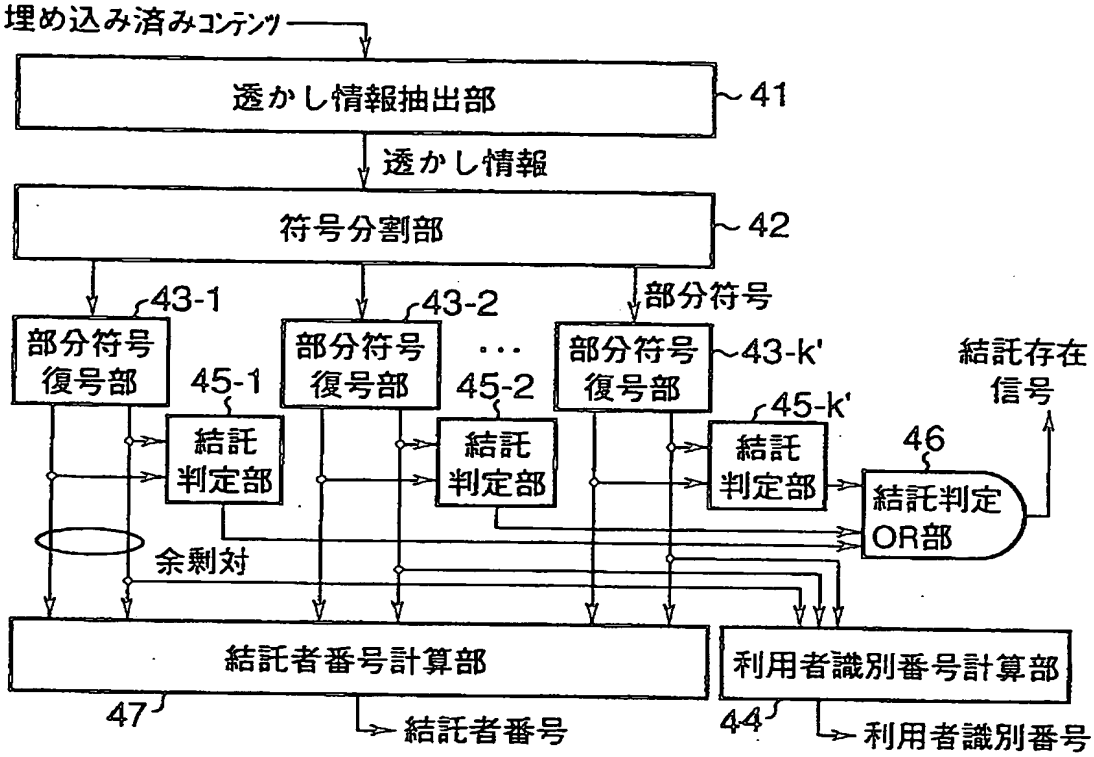
【図３】


21-k'
22-k'
24-k'
25
法記憶部
剰余計算部
部分符号生成部
符号連接部
透かし情報(埋め込み符号)
21-2
22-2
24-2
21-1
22-1
24-1
利用者識別番号
23
符号パラメータ記憶部

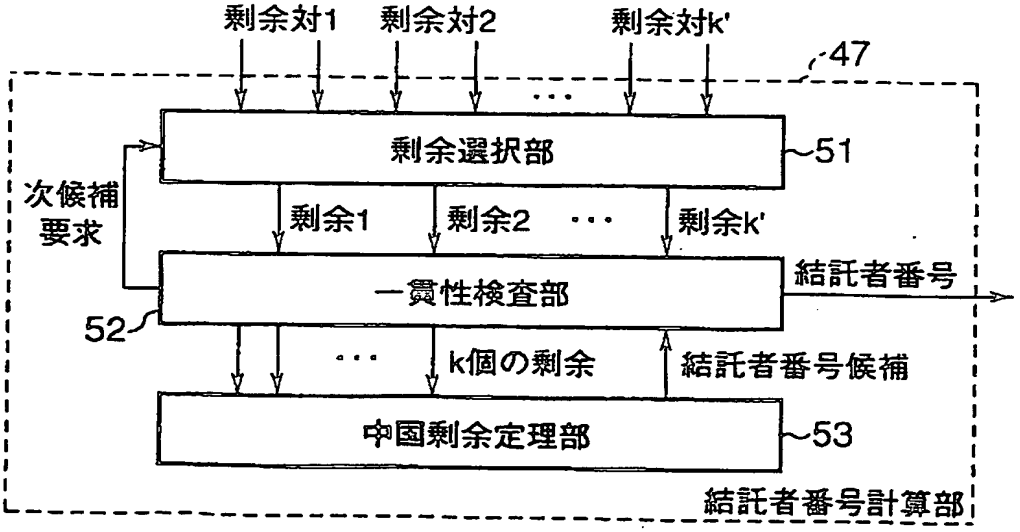
【図４】


符号
パラメータ
剰余
法
d
u_i
p_i
24-i
減算部
31
$p_i - u_i - 1$
"1"列生成部
33
$dX(p_i - u_i - 1)$ビットの"1"列
"0"列生成部
32
dXu_iビットの"0"列
連接部
34
$dX(p_i - 1)$ビットのビット列
部分符号生成部
部分符号

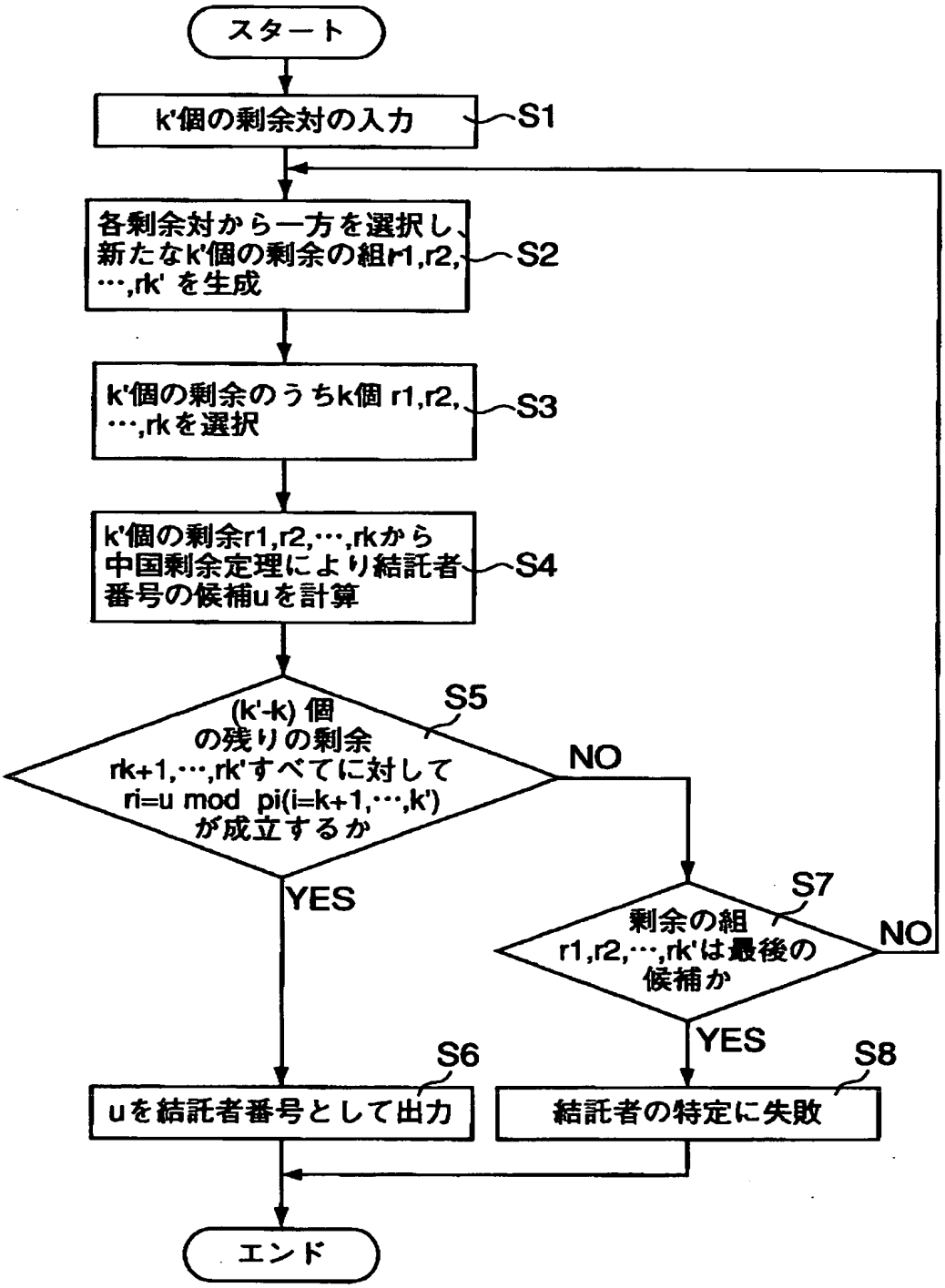
【図５】


埋め込み済みコンテンツ
透かし情報抽出部
41
透かし情報
符号分割部
42
部分符号
43-1
43-2
43-k'
部分符号復号部
45-1
45-2
45-k'
結託判定部
結託存在信号
46
結託判定OR部
余剰対
結託者番号計算部
47
結託者番号
利用者識別番号計算部
44
利用者識別番号

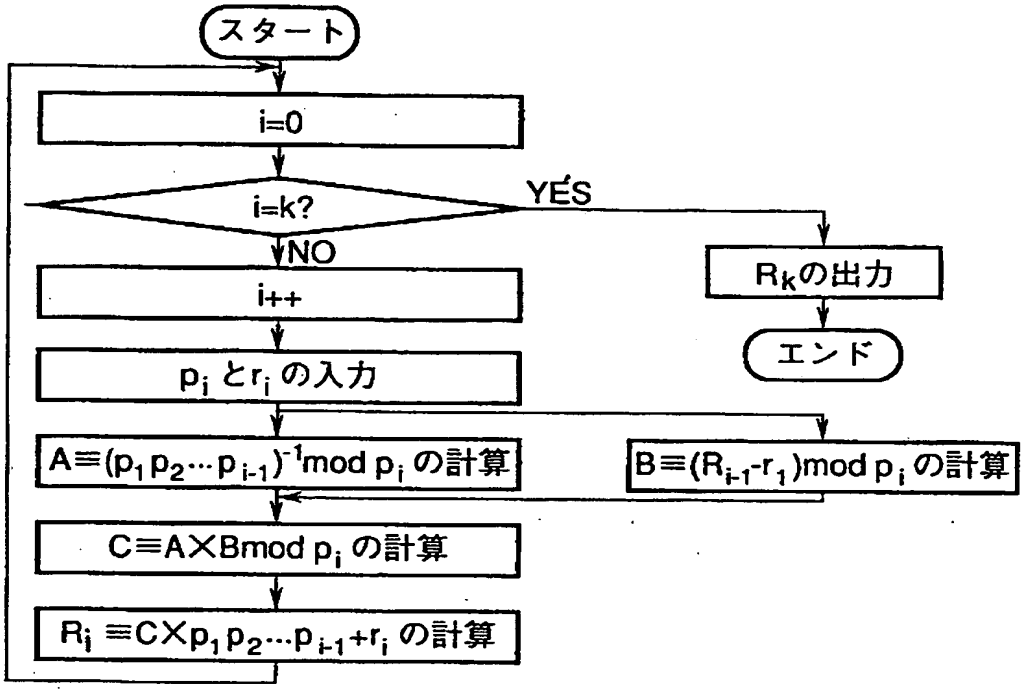
【図６】


剰余対1
剰余対2
剰余対k'
47
剰余選択部
51
次候補要求
剰余1
剰余2
剰余k'
一貫性検査部
結託者番号
52
k個の剰余
結託者番号候補
中国剰余定理部
53
結託者番号計算部

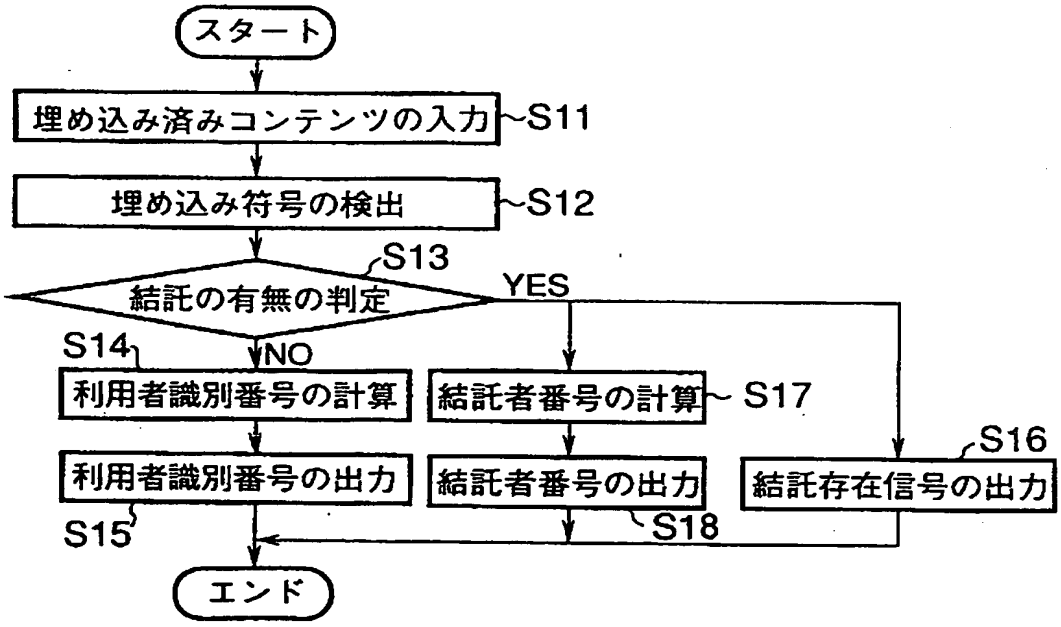
【図７】


スタート
k'個の剰余対の入力
S1
各剰余対から一方を選択し、新たなk'個の剰余の組r1,r2,…,rk' を生成
S2
k'個の剰余のうちk個 r1,r2,…,rkを選択
S3
k'個の剰余r1,r2,…,rkから中国剰余定理により結託者番号の候補uを計算
S4
(k'-k) 個の残りの剰余 rk+1,…,rk'すべてに対して ri=u mod pi(i=k+1,…,k') が成立するか
S5
NO
YES
剰余の組 r1,r2,…,rk'は最後の候補か
S7
NO
YES
uを結託者番号として出力
S6
結託者の特定に失敗
S8
エンド

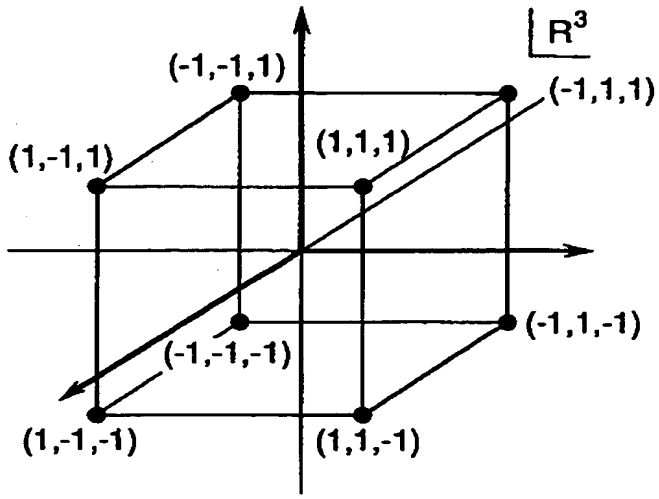
【図８】


スタート
i=0
i=k?
YES
NO
R_kの出力
エンド
i++
p_i とr_i の入力
$A \equiv (p_1 p_2 \cdots p_{i-1})^{-1} \bmod p_i$ の計算
$B \equiv (R_{i-1} - r_1) \bmod p_i$ の計算
$C \equiv A \times B \bmod p_i$ の計算
$R_i \equiv C \times p_1 p_2 \cdots p_{i-1} + r_i$ の計算

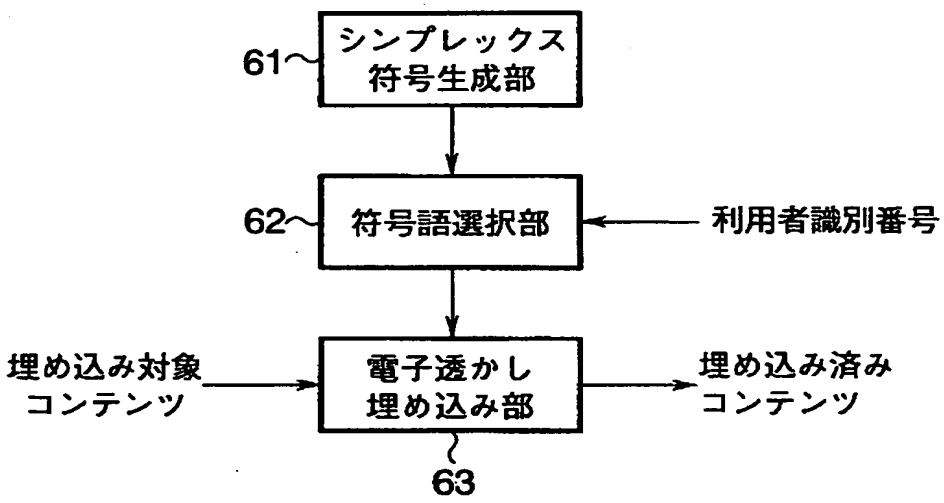
【図９】


スタート
埋め込み済みコンテンツの入力
S11
埋め込み符号の検出
S12
S13
結託の有無の判定
YES
NO
S14
利用者識別番号の計算
結託者番号の計算
S17
S16
利用者識別番号の出力
結託者番号の出力
結託存在信号の出力
S15
S18
エンド

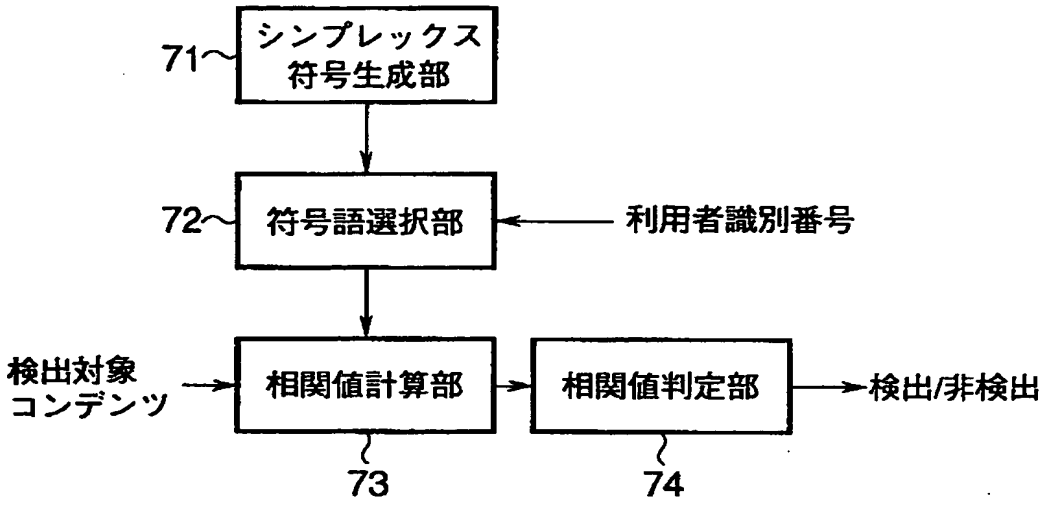
【図１０】


R3
(-1,-1,1)
(-1,1,1)
(1,-1,1)
(1,1,1)
(-1,1,-1)
(-1,-1,-1)
(1,-1,-1)
(1,1,-1)

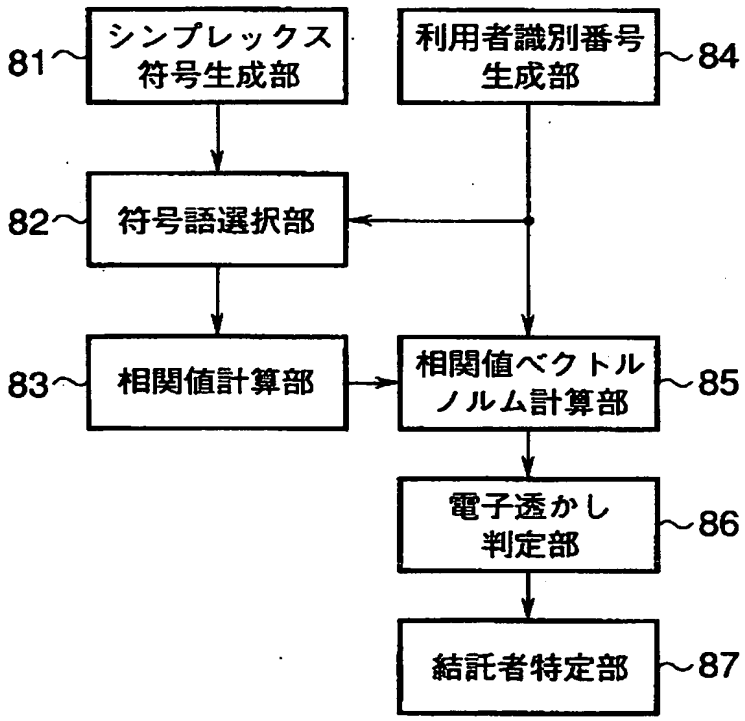
【図１１】


61
シンプレックス
符号生成部
62
符号語選択部
利用者識別番号
埋め込み対象
コンテンツ
電子透かし
埋め込み部
埋め込み済み
コンテンツ
63

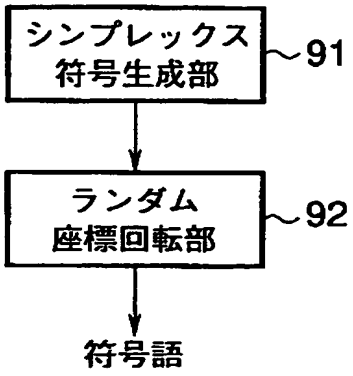
【図１２】


71
シンプレックス
符号生成部
72
符号語選択部
利用者識別番号
検出対象
コンデンツ
相関値計算部
相関値判定部
検出/非検出
73
74

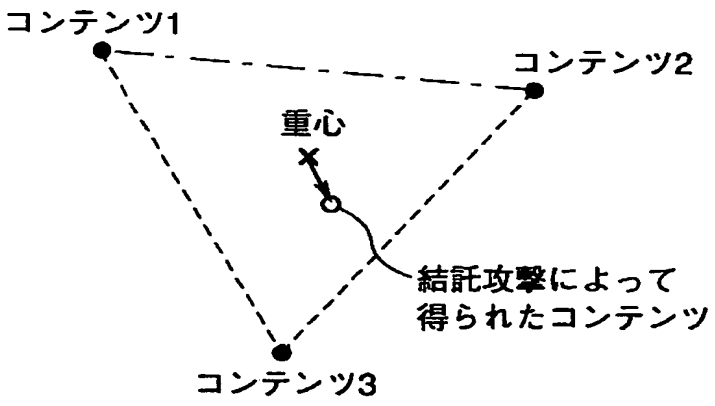
【図１３】


81
シンプレックス
符号生成部
利用者識別番号
生成部
84
82
符号語選択部
83
相関値計算部
相関値ベクトル
ノルム計算部
85
電子透かし
判定部
86
結託者特定部
87

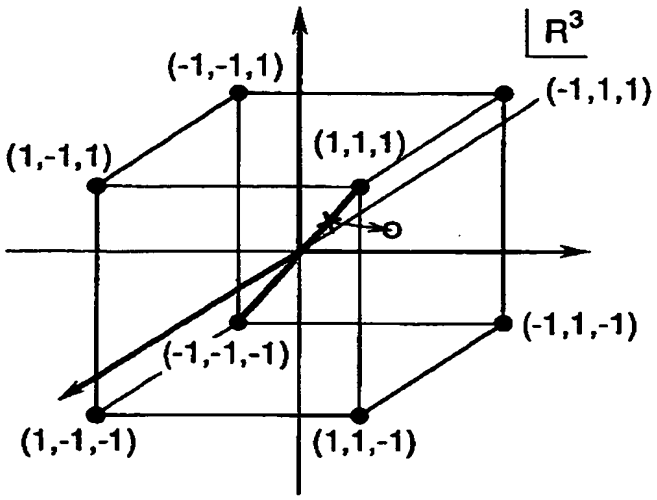
【図１４】


シンプレックス
符号生成部
91
ランダム
座標回転部
92
符号語

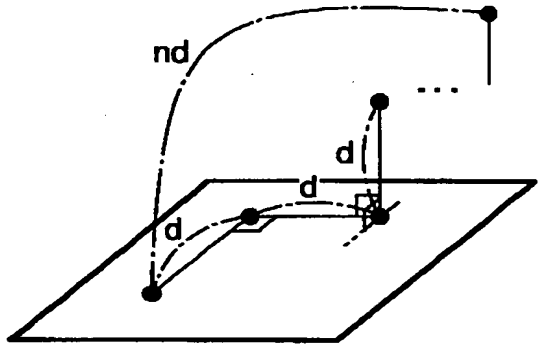
【図１５】


コンテンツ1
コンテンツ2
重心
結託攻撃によって
得られたコンテンツ
コンテンツ3

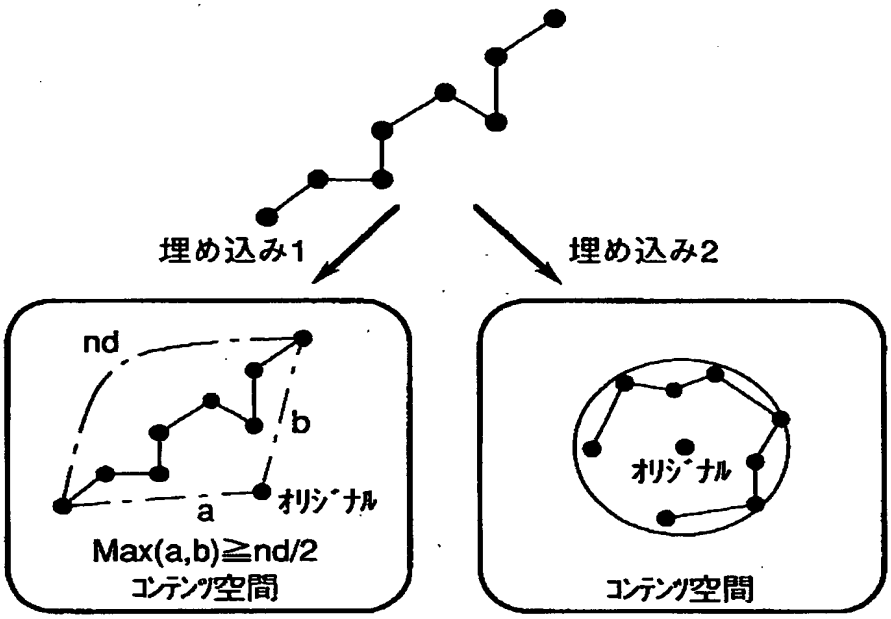
【図１６】



【図１７】



【図１８】



出証特２０００－３０４４２５９

【書類名】　　要約書

【要約】

【課題】結託攻撃への耐性を持ち、利用者総数や結託者総数が大きな場合においても、コンテンツの品質劣化を極力抑えて透かし情報を埋め込む電子透かし埋め込み装置を提供する。

【解決手段】剰余計算部２２－１，２２－２，…，２２－ｋ′により利用者識別番号に対して法記憶部２１－１，２１－２，…，２１－ｋ′に記憶された複数の素数を法とする剰余をそれぞれ求め、これらの剰余及び符号化パラメータ記憶部２３に記憶されたパラメータに基づいて、部分符号生成部２４－１，２４－２，…，２４－ｋ′により所定のビット数を一単位とする連続した１の列及び０の列で構成される部分符号をそれぞれ生成し、これらの各部分符号を連接部２５で連接して、透かし情報を構成する埋め込み符号を生成する。

【選択図】　　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
　［変更理由］　　新規登録
　　住　所　　神奈川県川崎市幸区堀川町７２番地
　　氏　名　　株式会社東芝